

The detailed autocorrelation distribution and 2-adic complexity of a classes of binary sequences with almost optimal autocorrelation

Yuhua Sun^{1,2,3}, Qiang Wang², Tongjiang Yan^{1,3}

¹ College of Sciences, China University of Petroleum,
Qingdao 266555, Shandong, China

² School of Mathematics and Statistics,
Carleton University, Ottawa , Ontario, K1S 5B6, Canada

³ Key Laboratory of Network Security and Cryptology,
Fujian Normal University, Fuzhou, Fujian 350117, China

Email: sunyuhua_1@163.com; wang@math.carleton.ca; yantoji@163.com

March 21, 2017

Abstract

Pseudo-random sequences with good statistical property, such as low autocorrelation, high linear complexity and large 2-adic complexity, have been used in designing reliable stream ciphers. In this paper, we obtain the exact autocorrelation distribution of a class of sequence with three-level autocorrelation and analyze the 2-adic complexity of this sequence. Our results show that the 2-adic complexity of the sequence is at least $(N + 1) - \log_2(N + 1)$ and that in many cases it is maximal, which is large enough to resist the attack of the rational approximation algorithm (RAA) for feedback with carry shift registers (FCSRs).

Index Terms. stream ciphers; pseudo-random sequences; autocorrelation; 2-adic complexity;

1 INTRODUCTION

Pseudo-random sequences with good statistical property are widely used as basic blocks for constructing stream ciphers. Any key stream generators could be implemented by both linear feedback shift registers (LFSRs) and feedback with carry shift registers (FCSRs). However, after the Berlekamp-Massey algorithm (BMA) for LFSRs [13] and the rational approximation algorithm for FCSRs [10] were presented, linear complexity and 2-adic complexity of the key stream sequence have been regarded as the critical

¹The work is supported by Shandong Provincial Natural Science Foundation of China(No. ZR2014FQ005, The Fundamental Research Funds for the Central Universities(No. 15CX02065A, No. 15CX08011A, No. 15CX02056A, No. 16CX02013A, No. 16CX02009A), Fujian Provincial Key Laboratory of Network Security and Cryptology Research Fund(Fujian Normal University)(No.15002).

security criteria and required to be no less than one half of the period. Autocorrelation is another critical statistical measure of the key stream sequence. Although the linear complexity of many classes of sequences have been obtained (See [3]-[4]), there are only a handful research papers that focus on 2-adic complexity. For example, in 1997, Klapper has pointed out that an m -sequence with prime period has maximal 2-adic complexity [10]. In 2010, Tian and Qi showed that the 2-adic complexity of all the binary m -sequences is maximal [17]. Afterwards, Xiong et al. [22] presented a new method of circulant matrices to compute the 2-adic complexities of binary sequences.

Several recent results show that the 2-adic complexity of a sequence possesses a close relationship with its another critical statistical property (i.e., autocorrelation). In [22], Xiong et al showed that all the known sequences with ideal 2-level autocorrelation have maximum 2-adic complexity. Moreover, in [2], Ding et al proved that the 2-adic complexities of Legendre sequences and Ding-Helleseth-Lam sequences with optimal autocorrelation are also maximal. Then, using the same method as that in [22], Xiong et al. [23] pointed out that two other classes of sequences based on interleaved structure have also maximal 2-adic complexity. One of these two classes of sequences was constructed by Tang and Ding [15], which has optimal autocorrelation, the other was constructed by Zhou et al [24], which is optimal with respect to the Tang-Fan-Matsufuji bound [16]. Recently, Hu [7] presented a simpler method to obtain the results of Xiong et al. [22], using detailed autocorrelation values.

In [1], Cai and Ding gave a generic construction of a large class of sequences with almost optimal autocorrelation, using almost difference sets. Then Wang [18] and Sun et al [14] proved that most of these sequences have high linear complexity. Meanwhile, Sun et al [14] generalized Cai and Ding's construction using d -form function with difference-balanced property and obtained more sequences with almost optimal autocorrelation in this way. In this paper, motivated by Hu's method [7], we determine the exact autocorrelation distribution and obtain a lower bound on the 2-adic complexity of these sequences. Our result shows that the low bound for this class of sequences with period N is at least $(N+1) - \log_2(N+1)$ and that in many cases it is maximal, which is large enough to resist against the rational approximation algorithm (RAA) attack for feedback with carry shift registers (FCSRs).

The rest of this paper is organized as follows. Some necessary definitions, notations, and previous results are introduced in Section 2. The exact autocorrelation distribution of a class of almost optimal autocorrelation sequences that generalized from Cai and Ding [1] by Sun et al [14] is given in Section 3. In Section 4, the lower bounds on the 2-adic complexities of these sequences will be presented. Finally we summarize our results and give some remarks in Section 5.

2 Preliminaries

Let N be a positive integer and $s = (s_0, s_1, \dots, s_{N-1})$ a binary sequence of period N . Let $S(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{Z}[x]$. Then we write

$$\frac{S(2)}{2^N - 1} = \frac{\sum_{i=0}^{N-1} s_i 2^i}{2^N - 1} = \frac{p}{q}, \quad 0 \leq p \leq q, \quad \gcd(p, q) = 1. \quad (1)$$

The 2-adic complexity $\Phi_2(s)$ of the sequence s is the integer $\lfloor \log_2 q \rfloor$, i.e.,

$$\Phi_2(s) = \left\lfloor \log_2 \frac{2^N - 1}{\gcd(2^N - 1, S(2))} \right\rfloor, \quad (2)$$

where $\lfloor x \rfloor$ is the greatest integer that is less than or equal to x .

Let $C = \{0 \leq i \leq N-1 : s_i = 1\}$ be the support of s . Then s is called the characteristic sequence of C . The autocorrelation of s is defined by

$$AC(\tau) = \sum_{i=0}^{N-1} (-1)^{s_i + s_{i+\tau}}, \quad \tau = 0, 1, 2, \dots, N-1, \quad (3)$$

where $\tau \in \mathbb{Z}_N$. It is well known that $AC(\tau) \equiv N \pmod{4}$ for all $\tau \in \mathbb{Z}_N$. Moreover, it can be computed by

$$AC(\tau) = N - 4(|C| - d_C(\tau)), \quad (4)$$

where $d_C(\tau)$ is the difference function of the support C such that $\tau + C = \{\tau + i \mid i \in C\}$ and

$$d_C(\tau) = |C \cap (\tau + C)|. \quad (5)$$

Definition 1 Let $(G, +)$ be a cyclic group with N elements and C be a k -element subset of G . Supposing the variable τ ranges over all the nonzero elements of G . If $d_C(\tau)$ always takes on the value λ , then C is called a (N, k, λ) cyclic difference set of G ; if $d_C(\tau)$ takes on λ altogether t times and $\lambda + 1$ altogether $N - 1 - t$ times, then C is called a (N, k, λ, t) cyclic almost difference set (CADS) in G .

According to Eq. (4), when the support C of a sequence s is a (N, k, λ, t) cyclic almost difference set, the autocorrelation of s is

$$AC(\tau) = \begin{cases} N, & \text{for 1 time,} \\ N - 4(k - \lambda), & \text{for } t \text{ times,} \\ N - 4(k - \lambda - 1), & \text{for } N - 1 - t \text{ times.} \end{cases} \quad (6)$$

Therefore, under the assumption $N \equiv 3 \pmod{4}$), a sequence s of period N has almost optimal autocorrelation if and only if $AC(\tau) = -1$ or 3 for all $\tau \not\equiv 0 \pmod{N}$ (see [1]).

Let q be a power of a prime and n a positive integer.

Definition 2 A function f from \mathbb{F}_{q^n} to \mathbb{F}_q is called a d -form function on \mathbb{F}_{q^n} over \mathbb{F}_q if $f(xy) = y^d f(x)$ for any $x \in \mathbb{F}_{q^n}$ and $y \in \mathbb{F}_q$.

Definition 3 A function from \mathbb{F}_{q^n} to \mathbb{F}_q is said to be balanced if the element 0 appears one less time than each nonzero element in \mathbb{F}_q in the list $f(\alpha^0), f(\alpha^1), \dots, f(\alpha^{q^n-2})$, where α is a primitive element of \mathbb{F}_{q^n} .

Definition 4 Let $f(x)$ be a d -form function on \mathbb{F}_{q^n} over \mathbb{F}_q and $\gcd(d, q^n - 1) = 1$. Then the function $f(x)$ is called difference-balanced if $f(xz) - f(x)$ is balanced for any $z \in \mathbb{F}_{q^n} \setminus \{1\}$.

Earlier, Sun et al [14] extended Cai and Ding's construction [1] to obtain the following almost difference sets.

Lemma 1 [14] Let m be a positive integer, α a primitive element of the finite field $\mathbb{F}_{2^{2m}}$ and $f(x)$ a d -form function from $\mathbb{F}_{2^{2m}}$ to \mathbb{F}_{2^m} with difference-balanced property. Suppose that C'_1 is any $(2^m - 1, 2^{m-1} - 1, 2^{m-2} - 1)$ difference set in $(\mathbb{Z}_{2^m-1}, +)$. Define $C_1 = \{(2^m + 1)i \mid i \in C'_1\}$, $C_2 = \{i \in \mathbb{Z}_{2^{2m}-1} \mid f(\alpha^i) = 1\}$, $C = C_1 + C_2 = \{(c_1 + c_2) \pmod{2^{2m} - 1} \mid c_1 \in C_1, c_2 \in C_2\}$. Then C is a $(2^{2m} - 1, 2^{2m-1} - 2^m, 2^{2m-2} - 2^m, 2^m - 2)$ almost difference set in $(\mathbb{Z}_{2^{2m}-1}, +)$. Furthermore, the characteristic sequence of the set C has the out-of-phase autocorrelation values $\{-1, 3\}$ only.

In the sequel, we also need the following number theoretical results.

Definition 5 A composite number n is called a 2-pseudoprime if $2^{n-1} \equiv 1 \pmod{n}$.

For example, both $341 = 11 \cdot 31$ and $561 = 3 \cdot 11 \cdot 17$ are 2-pseudoprimes.

Lemma 2 [11] If n is a 2-pseudoprime, then $2^n - 1$ is a 2-pseudoprime. Therefore, there are infinitely many 2-pseudoprimes.

3 Detailed autocorrelation distribution of sequences generalized from Cai and Ding by Sun et al.

In this section, we derive the exact autocorrelation distribution of the sequence s constructed in Lemma 1. Previously, we know that the autocorrelation of this sequence is almost optimal, however, it is not good enough to help us determine the lower bound on its 2-adic complexity. In order to achieve our goal, we use Eq. (6) and Lemma 1 to find out the exact autocorrelation distribution of s .

Lemma 3 Let $f(x)$ be a d -form function on \mathbb{F}_{q^n} over \mathbb{F}_q with difference-balanced property. Define $H_a = \{x \in \mathbb{F}_{q^n}^* \mid f(x) = a, a \in \mathbb{F}_q^*\}$. Then, for a primitive element β of \mathbb{F}_q and $i \in \{1, 2, \dots, q-2\}$, we must have $\beta^i x \notin H_a$ for any $x \in H_a$ and $|H_a| = q^{n-1}$.

Proof. By the definition of d -form function, $f(\beta^i x) = \beta^{id} f(x)$ for any $x \in \mathbb{F}_{q^n}$. If $x \in H_a$ and $\beta^i x \in H_a$, we get $\beta^{id} = 1$, which is impossible since $\gcd(d, q-1) = 1$ and $i \in \{1, 2, \dots, q-2\}$. Additionally, the difference-balanced property guarantees $|H_a| = q^{n-1}$.

Lemma 4 Let all the symbols be the same as those in Lemma 1. Suppose that $\tau = (2^m + 1)\tau_1$, where $\tau_1 \in \{1, 2, \dots, 2^m - 2\}$. Then

$$d_C(\tau) = |C \cap (C + \tau)| = 2^{2m-2} - 2^m.$$

Proof. Let $c_1 = (2^m + 1)i$ with a fixed $i \in C'_1$ such that $i + \tau_1 \in C'_1$. Then, for any $c_2 \in C_2$, we can see that $c = c_1 + c_2 \in C$ and $c + \tau = c_1 + c_2 + \tau = (2^m + 1)(i + \tau_1) + c_2 \in C$. Conversely, for any $c \in C$, the pair (c_1, c_2) such that $c = c_1 + c_2$ with $c_1 \in C_1$ and $c_2 \in C_2$ is unique. Moreover, there exists exactly one $i \in C'_1$ such that $c_1 = (2^m + 1)i$ and $c + \tau = (2^m + 1)(i + \tau_1) + c_2 \in C$. Indeed, by the first conclusion of Lemma 3, $c_2 + (2^m + 1)k \notin C_2$ for any $c_2 \in C_2$ and any $k \in \{1, 2, \dots, 2^m - 2\}$. Therefore, $c = c_1 + c_2 \in C$ and $c + \tau \in C$ if and only if $(2^m + 1)(i + \tau_1) \in C_1$, i.e., $i + \tau_1 \in C'_1$.

Hence,

$$d_C(\tau) = |C \cap (C + \tau)| = |C_2| \cdot |C'_1 \cap (C'_1 + \tau_1)| = |C_2| \cdot d_{C'_1}.$$

By the assumption that C'_1 is a $(2^m - 1, 2^{m-1} - 1, 2^{m-2} - 1)$ difference set in $(\mathbb{Z}_{2^m-1}, +)$. Then $d_{C'_1} = 2^{m-2} - 1$. Furthermore, $|C_2| = 2^m$ by Lemma 3. The result follows.

Theorem 1 Let m be a positive integer, α a primitive element of $\mathbb{F}_{2^{2m}}$ and $f(x)$ a d -form function from $\mathbb{F}_{2^{2m}}$ to \mathbb{F}_{2^m} with difference-balanced property. Suppose that C'_1 is any $(2^m - 1, 2^{m-1} - 1, 2^{m-2} - 1)$ difference set in $(\mathbb{Z}_{2^m-1}, +)$. Define $C_1 = \{(2^m + 1)i \mid i \in C'_1\}$, $C_2 = \{i \in \mathbb{Z}_{2^{2m}-1} \mid f(\alpha^i) = 1\}$, $C = C_1 + C_2 = \{(c_1 + c_2) \pmod{2^{2m}-1} \mid c_1 \in C_1, c_2 \in C_2\}$. Then the exact autocorrelation distribution of the characteristic sequence s of C is given by

$$AC(\tau) = \begin{cases} -1, & \tau \in \{(2^m + 1)\tau_1 \mid \tau_1 = 1, 2, \dots, 2^m - 2\}, \\ 3, & 1 \leq \tau \leq 2^{2m} - 2, \text{ but } \tau \notin \{(2^m + 1)\tau_1 \mid \tau_1 = 1, 2, \dots, 2^m - 2\}. \end{cases}$$

Proof. First of all, from the parameters of the almost difference set C in Lemma 1, we know that $|C| = 2^{2m-1} - 2^m$ and that there are $2^m - 2$ τ 's such that the autocorrelation $AC(\tau) = -1$. Secondly, by Lemma 4 we have $d_C(\tau) = |C \cap (C + \tau)| = 2^{2m-2} - 2^m$ for $\tau \in \{(2^m + 1)\tau_1 \mid \tau_1 = 1, 2, \dots, 2^m - 2\}$. Then, using Eq. (4), we get $AC(\tau) = -1$ for $\tau \in \{(2^m + 1)\tau_1 \mid \tau_1 = 1, 2, \dots, 2^m - 2\}$. Note that the size of the set $\{(2^m + 1)\tau_1 \mid \tau_1 = 1, 2, \dots, 2^m - 2\}$ is exactly $2^m - 2$. Therefore the proof is complete.

4 Lower bounds on the 2-adic complexity of sequences generalized from Cai and Ding by Sun et al.

Recall that the sequence s in Lemma 1 has the period $N = 2^{2m} - 1$. In the following we let $S(x) = \sum_{i=0}^{N-1} s_i x^i$ and $T(x) = \sum_{i=0}^{N-1} (-1)^{s_i} x^i \in \mathbb{Z}[x]$.

Lemma 5 *Let $S(x) = \sum_{i=0}^{N-1} s_i x^i$ and $T(x) = \sum_{i=0}^{N-1} (-1)^{s_i} x^i \in \mathbb{Z}[x]$. Then*

$$-2S(x)T(x^{-1}) \equiv N + \sum_{\tau=1}^{N-1} AC(\tau)x^\tau - T(x^{-1}) \left(\sum_{i=0}^{N-1} x^i \right) \pmod{x^N - 1}. \quad (7)$$

proof. According to the definition of $T(x)$, we have

$$\begin{aligned} T(x)T(x^{-1}) &\equiv \left(\sum_{i=0}^{N-1} (-1)^{s_i} x^i \right) \left(\sum_{j=0}^{N-1} (-1)^{s_j} x^{-j} \right) \pmod{x^N - 1} \\ &\equiv \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} (-1)^{s_i + s_j} x^{i-j} \pmod{x^N - 1} \\ &\equiv N + \sum_{\tau=1}^{N-1} \sum_{j=0}^{N-1} (-1)^{s_{j+\tau} + s_j} x^\tau \pmod{x^N - 1} \\ &\equiv N + \sum_{\tau=1}^{N-1} AC(\tau)x^\tau \pmod{x^N - 1}. \end{aligned} \quad (8)$$

Furthermore, we have

$$T(x) = \sum_{i=0}^{N-1} (-1)^{s_i} x^i = \sum_{i=0}^{N-1} (1 - 2s_i)x^i = \sum_{i=0}^{N-1} x^i - 2S(x). \quad (9)$$

Combining Eqs. (8)–(9), we obtain the result. \square

Employing Lemma 5 and the detailed autocorrelation distribution of s , we can obtain the following.

Lemma 6 *Let m be a positive integer, $N = 2^{2m} - 1$, and s be the binary sequence with almost optimal autocorrelation in Lemma 1. Then*

$$S(2)T(2^{-1}) \equiv -2 \left(2^{2m-2} - \frac{2^N - 1}{2^{2m+1} - 1} \right) \pmod{2^N - 1}. \quad (10)$$

proof. Recall that $C_1 = \{(2^m + 1)\tau_1 | \tau_1 = 1, 2, \dots, 2^m - 2\}$ in Lemma 5. In convenience, we denote $\mathbf{Z}_N^* = \{1, 2, \dots, N - 1\}$. Substituting the autocorrelation in Theorem 1 into Eq. (7) in Lemma 5, we can see

$$\begin{aligned}
-2S(x)T(x^{-1}) &\equiv N + \sum_{\tau=1}^{N-1} AC(\tau)x^\tau - T(x^{-1}) \left(\sum_{i=0}^{N-1} x^i \right) \pmod{x^N - 1} \\
&\equiv N + \sum_{\tau \in \mathbf{Z}_N^* \setminus C_1} 3 \cdot x^\tau + \sum_{\tau \in C_1} (-1) \cdot x^\tau \\
&\quad - T(x^{-1}) \left(\sum_{i=0}^{N-1} x^i \right) \pmod{x^N - 1} \\
&\equiv N + \sum_{\tau \in \mathbf{Z}_N^*} 3 \cdot x^\tau + \sum_{\tau \in C_1} (-3) \cdot x^\tau + \sum_{\tau \in C_1} (-1) \cdot x^\tau \\
&\quad - T(x^{-1}) \left(\sum_{i=0}^{N-1} x^i \right) \pmod{x^N - 1} \\
&\equiv N + \sum_{\tau \in \mathbf{Z}_N^*} 3 \cdot x^\tau + \sum_{\tau \in C_1} (-4) \cdot x^\tau \tag{11} \\
&\quad - T(x^{-1}) \left(\sum_{i=0}^{N-1} x^i \right) \pmod{x^N - 1} \\
&\equiv N + \sum_{\tau=1}^{N-1} 3 \cdot x^\tau + \sum_{\tau_1=1}^{2^m-2} (-4) \cdot x^{(2^m+1)\tau_1} \\
&\quad - T(x^{-1}) \left(\sum_{i=0}^{N-1} x^i \right) \pmod{x^N - 1} \\
&\equiv N - 3 \left(1 - \sum_{\tau=0}^{N-1} x^\tau \right) + \left(4 - 4 \cdot \sum_{\tau_1=0}^{2^m-2} x^{(2^m+1)\tau_1} \right) \\
&\quad - T(x^{-1}) \left(\sum_{i=0}^{N-1} x^i \right) \pmod{x^N - 1} \\
&\equiv N + 1 - \frac{4(x^N - 1)}{x^{2^m+1} - 1} - (1 + T(x^{-1})) \left(\sum_{i=0}^{N-1} x^i \right) \pmod{x^N - 1}.
\end{aligned}$$

Then, substituting 2 for x we have

$$\begin{aligned} -2S(2)T(2^{-1}) &\equiv N + 1 - \frac{4(2^N - 1)}{2^{2^m+1} - 1} \pmod{2^N - 1} \\ &\equiv 4 \left(2^{2^m-2} - \frac{2^N - 1}{2^{2^m+1} - 1} \right) \pmod{2^N - 1}. \end{aligned}$$

The result follows. \square

In order to give the lower bound on the 2-adic complexity, we also need the following simple result in number theory whose proof is omitted here.

Lemma 7 *Let n', m' be any positive integer. Then*

$$\frac{2^{n'm'} - 1}{2^{m'} - 1} \equiv n' \pmod{2^{m'} - 1}.$$

Now we give a general lower bound on the 2-adic complexity for the sequence s constructed in Lemma 1.

Theorem 2 *Let m be a positive integer, α a primitive element of $\mathbb{F}_{2^{2m}}$ and $f(x)$ a d -form function from $\mathbb{F}_{2^{2m}}$ to \mathbb{F}_{2^m} with difference-balanced property. Suppose that C'_1 is any $(2^m - 1, 2^{m-1} - 1, 2^{m-2} - 1)$ difference set in $(\mathbb{Z}_{2^m-1}, +)$, $C_1 = \{(2^m + 1)i | i \in C'_1\}$, $C_2 = \{i \in \mathbb{Z}_{2^{2m}-1} | f(\alpha^i) = 1\}$ and $C = C_1 + C_2 = \{(c_1 + c_2) \pmod{(2^{2m} - 1)} | c_1 \in C_1, c_2 \in C_2\}$. Denote s to be the characteristic sequence of C . Then the 2-adic complexity $\Phi_2(s)$ of s is bounded by*

$$\Phi_2(s) \geq (N + 1) - \log_2(N + 1). \quad (12)$$

Proof. Above all, from the known conditions, we know that $m \geq 2$. It is easy to see that

$$\gcd(S(2), 2^N - 1) | \gcd(S(2)T(2^{-1}), 2^N - 1)$$

and that the product

$$\gcd\left(S(2)T(2^{-1}), \frac{2^N - 1}{2^{2^m+1} - 1}\right) \gcd\left(S(2)T(2^{-1}), 2^{2^m+1} - 1\right)$$

is divided by $\gcd(S(2)T(2^{-1}), 2^N - 1)$. Then we get

$$\begin{aligned} \gcd(S(2), 2^N - 1) &| \left(\gcd\left(S(2)T(2^{-1}), \frac{2^N - 1}{2^{2^m+1} - 1}\right) \right. \\ &\quad \left. \gcd\left(S(2)T(2^{-1}), 2^{2^m+1} - 1\right) \right). \end{aligned} \quad (13)$$

By Lemma 6, we have

$$\begin{aligned} S(2)T(2^{-1}) &\equiv -2(2^{2m-2} - \frac{2^N - 1}{2^{2m+1} - 1}) \pmod{2^N - 1} \\ &\equiv -2^{2m-1} \pmod{\frac{2^N - 1}{2^{2m+1} - 1}}. \end{aligned}$$

Then we have

$$\gcd(S(2)T(2^{-1}), \frac{2^N - 1}{2^{2m+1} - 1}) = \gcd(2^{2m-1}, \frac{2^N - 1}{2^{2m+1} - 1}) = 1. \quad (14)$$

Upper bound of $\gcd(S(2)T(2^{-1}), 2^{2^m+1} - 1)$ is considered in the following. Note that $N = 2^{2^m} - 1 = (2^m - 1)(2^m + 1)$. By Lemma 7, we get

$$\frac{2^N - 1}{2^{2^m+1} - 1} \equiv 2^m - 1 \pmod{2^{2^m+1} - 1}.$$

Then, by Lemma 6 again, we have

$$\begin{aligned} S(2)T(2^{-1}) &\equiv -2 \left(2^{2m-2} - \frac{2^N - 1}{2^{2m+1} - 1} \right) \pmod{2^N - 1} \\ &\equiv -2(2^{2m-2} - 2^m + 1) \pmod{2^{2^m+1} - 1} \end{aligned}$$

Accordingly, we know that

$$\gcd(S(2)T(2^{-1}), 2^{2^m+1} - 1) = \gcd(2^{2m-2} - 2^m + 1, 2^{2^m+1} - 1). \quad (15)$$

Note that

$$2^{2m-2} - 2^m + 1 < 2^{2m-2} + 1 < 2^{2^m+1} - 1 \quad (m \geq 2).$$

Therefore we obtain an upper bound of $\gcd(S(2)T(2^{-1}), 2^{2^m+1} - 1)$

$$\gcd(S(2)T(2^{-1}), 2^{2^m+1} - 1) \leq 2^{2m-2} - 2^m + 1 < 2^{2m-2} - 1. \quad (16)$$

Combining Eqs. (13),(14) and (16), we have

$$\gcd(S(2), 2^N - 1) \leq 2^{2(m-1)} - 1.$$

Therefore, by Eq. (2), the 2-adic complexity $\Phi_2(s)$ of s is bounded by

$$\begin{aligned} \Phi_2(s) &= \lfloor \log_2 \frac{2^N - 1}{\gcd(S(2), 2^N - 1)} \rfloor \geq (N - 1) - 2(m - 1) \\ &= N - 2m + 1 = (N + 1) - \log_2(N + 1). \end{aligned}$$

□

Remark 1 From the result of Theorem 2, it is easy to test that the lower bound in Eq.(12) is larger than $\frac{N}{2}$ for any positive integer m . Hence, the 2-adic complexity of s is large enough to resist RAA. In fact, in many cases, the lower bound can be maximal. In the following, we will discuss these cases.

Lemma 8 Let $m - 1$ be a prime or a 2-pseudoprime. Then we have

$$\gcd\left(S(2)T(2^{-1}), 2^{2^m+1} - 1\right) = \begin{cases} 2^5 - 1, & \text{if } m - 1 \equiv 5 \pmod{20}, \\ 1, & \text{otherwise.} \end{cases}$$

Proof. Note that $2^{2^m-2} - 2^m + 1 = (2^{m-1} - 1)^2$. Then, by Eq. (15), we know that

$$\gcd\left(S(2)T(2^{-1}), 2^{2^m+1} - 1\right) = \gcd\left((2^{m-1} - 1)^2, 2^{2^m+1} - 1\right). \quad (17)$$

Next, we will determine the value of $\gcd(2^{m-1} - 1, 2^{2^m+1} - 1)$ in several steps.

Firstly, it is easy to see that

$$\gcd\left(2^{m-1} - 1, 2^{2^m+1} - 1\right) = 2^{\gcd(m-1, 2^m+1)} - 1. \quad (18)$$

Since $m - 1$ is a prime or a 2-pseudoprime, then we have $m - 1 \mid 2^{m-2} - 1$, which implies that $2^m + 1 = 4(2^{m-2} - 1) + 5 \equiv 5 \pmod{m - 1}$. Therefore, we have $\gcd(2^m + 1, m - 1) = \gcd(m - 1, 5)$. By Eq. (18), we know that

$$\gcd\left(2^{m-1} - 1, 2^{2^m+1} - 1\right) = \begin{cases} 2^5 - 1, & \text{if } m - 1 \equiv 0 \pmod{5}, \\ 1, & \text{otherwise.} \end{cases} \quad (19)$$

Secondly, we will prove $m - 1 \equiv 5 \pmod{10}$ if $5 \mid m - 1$, i.e., $m - 1$ is not even if $5 \mid m - 1$. Otherwise, if $m - 1$ is even, i.e., m is odd, then $m \equiv 1 \pmod{4}$ or $m \equiv 3 \pmod{4}$, which implies that $2^m \equiv 2 \pmod{5}$ if $m \equiv 1 \pmod{4}$ and $2^m \equiv 3 \pmod{5}$ if $m \equiv 3 \pmod{4}$. But since $m - 1$ is a prime or 2-pseudoprime, we have $m - 1 \mid 2^{m-2} - 1$. Further, since $5 \mid m - 1$, then $5 \mid 2^{m-2} - 1$ and $2^m = 4(2^{m-2} - 1) + 4 \equiv 4 \pmod{5}$, a contradiction to $2^m \equiv 2 \pmod{5}$ or $2^m \equiv 3 \pmod{5}$. Thus, we obtain that

$$\gcd(2^{m-1} - 1, 2^{2^m+1} - 1) = \begin{cases} 2^5 - 1, & \text{if } m - 1 \equiv 5 \pmod{10}, \\ 1, & \text{otherwise.} \end{cases}$$

Thirdly, we will prove $m - 1 \equiv 5 \pmod{20}$ if $m - 1 \equiv 5 \pmod{10}$, i.e., $m - 1 \not\equiv 15 \pmod{20}$ if $m - 1 \equiv 5 \pmod{10}$. Otherwise, if $m - 1 \equiv 15 \pmod{20}$, then we have $m - 1 \equiv 3 \pmod{4}$ or $m \equiv 0 \pmod{4}$, which implies $2^m \equiv 1 \pmod{5}$, a contradiction to the above $2^m = 4(2^{m-2} - 1) + 4 \equiv 4 \pmod{5}$. Thus we have

$$\gcd(2^{m-1} - 1, 2^{2^m+1} - 1) = \begin{cases} 2^5 - 1, & \text{if } m - 1 \equiv 5 \pmod{20}, \\ 1, & \text{otherwise.} \end{cases}$$

Now, we will prove that $2^{2^m+1} - 1$ is not divided by $(2^5 - 1)^2$ if $2^5 - 1 | 2^{2^m+1} - 1$. Otherwise, it is easy to see that $2^5 - 1 | 2^{2^m+1} - 1$, i.e., $5 | 2^m + 1$. Then, we have $2^{2^m+1} - 1 = (2^5 - 1) \times \frac{2^{2^m+1}-1}{2^5-1}$, which implies that $2^5 - 1 | \frac{2^{2^m+1}-1}{2^5-1}$. By Lemma 7, we have $\frac{2^{2^m+1}-1}{2^5-1} \equiv \frac{2^m+1}{5} \pmod{2^5-1}$. Then we can get $2^5 - 1 | 2^m + 1$. Therefore, we have $2^5 - 1 | 2^{2^m} - 1$, i.e., $5 | 2^m$, which implies $5 | m$, a contradiction to the fact $5 | m - 1$. Thus, by Eqs. (17) and (20), we know that Eq. (17) holds. The desired result follows. \square

Theorem 3 *Let m be a positive integer, $N = 2^{2^m} - 1$, α a primitive element of $\mathbb{F}_{2^{2^m}}$ and $f(x)$ a d -form function from $\mathbb{F}_{2^{2^m}}$ to \mathbb{F}_{2^m} with difference-balanced property. Suppose that C'_1 is any $(2^m - 1, 2^{m-1} - 1, 2^{m-2} - 1)$ difference set in $(\mathbb{Z}_{2^m-1}, +)$. Define $C_1 = \{(2^m+1)i | i \in C'_1\}$, $C_2 = \{i \in \mathbb{Z}_{2^{2^m}-1} | f(\alpha^i) = 1\}$, $C = C_1 + C_2 = \{(c_1 + c_2) \pmod{(2^{2^m} - 1)} | c_1 \in C_1, c_2 \in C_2\}$. Let s be the sequence whose support set is C . Then the 2-adic complexity $\Phi_2(s)$ of s is bounded by*

$$\Phi(s) \geq \begin{cases} N - 1, & \text{if } m - 1 \text{ is a prime or} \\ & \text{a 2-pseudoprime but } m - 1 \not\equiv 5 \pmod{20}, \\ N - 6, & \text{if } m - 1 \text{ is a prime or} \\ & \text{a 2-pseudoprime and } m - 1 \equiv 5 \pmod{20}, \\ (N + 1) - \log_2(N + 1), & \text{otherwise.} \end{cases}$$

Proof. From Eq. (2), the 2-adic complexity of s satisfies

$$\begin{aligned} \Phi(s) &= \lfloor \log_2 \frac{2^N - 1}{\gcd(S(2), 2^N - 1)} \rfloor \geq \lfloor \log_2 \frac{2^N - 1}{\gcd(S(2)T(2^{-1}), 2^N - 1)} \rfloor \\ &\geq \lfloor \log_2 \frac{2^N - 1}{\gcd(S(2)T(2^{-1}), 2^{2^m+1} - 1) \gcd(S(2)T(2^{-1}), \frac{2^N - 1}{2^{2^m+1} - 1})} \rfloor \end{aligned}$$

The rest of the proof is from Lemma 8 and the discussion in the proof of Theorem 2.

Remark 2 *From Theorem 3, the 2-adic complexity of the sequences with almost optimal autocorrelation is large enough to resist the analysis of RAA.*

5 Summary and concluding remarks

In this paper, we first gave the detailed autocorrelation distribution of the sequence with almost optimal autocorrelation generalized from Cai and Ding by Sun et al.. Then, using the the detailed autocorrelation distribution and combining the method of Hu and some number theory, we present the lower bounds on the 2-adic complexity of these sequences in the general case and some special cases respectively. Our results show that the 2-adic complexity is at least $(N + 1) - \log_2(N + 1)$ and that in many cases it is maximal, which is obviously large enough to resist RAA of FCSR.

References

- [1] Cai, Y., Ding, C.: Binary sequences with optimal autocorrelation. *Theoretical Computer Science* 410, 2316-2322 (2009).
- [2] Ding, C., Helleseht, T., Lam, K. Y.: Several classes of sequences with three-level autocorrelation. *IEEE Trans. Inf. Theory* 45, 2606-2612 (1999).
- [3] Ding, C., Helleseht, T., Shan, W.: On the linear complexity of Legendre sequences. *IEEE Trans. Inf. Theory* 45, 693-698 (1998).
- [4] Edemskiy, V., Palvinskiy, A.: The linear complexity of binary sequences of length $2p$ with optimal three-level autocorrelation. *Information Processing Letters* 116, 153-156 (2016).
- [5] Etzion, T.: Linear complexity of de Bruijn sequences-old and new results. *IEEE Trans. Inf. Theory* 45, 693-698 (1999).
- [6] Helleseht, T., Maas, M., Mathiassen, E., Segers, T.: Linear complexity over \mathbb{F}_p of Sidel'nikov sequences. *IEEE Trans. Inf. Theory* 50, 2468-2472 (2004).
- [7] Hu, H.: Comments on a new method to compute the 2-adic complexity of binary sequences. *IEEE Trans. Inf. Theory* 60, 5803-5804 (2014).
- [8] Hu, L., Yue, Q., Wang, M.: The linear complexity of whiteman's generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$. *IEEE Trans. Inf. Theory* 58, 5534-5543 (2012).
- [9] Kim, Y., Jang, J. W., Kim, S. H., No, J. S.: Linear complexity of quaternary sequences constructed from binary Legendre sequences. *International Symposium on Information Theory and Its Applications*, 611-614(2012).
- [10] Klapper, A., Goresky, M.: Feedback shift registers, 2-adic span, and combiners with memory. *Journal of Cryptology* 10, 111-147 (1997).
- [11] Kumanduri, R., Romero, C.: *Number theory with computer applications*. Prentice hall, upper Saddle River, New Jersey (1998).
- [12] Li, N., Tang, X.: On the linear complexity of binary sequences of period $4N$ with optimal autocorrelation/magnitude. *IEEE Trans. Inf. Theory* 57, 7597-7604 (2011).
- [13] Massey, J. L.: Shift-register synthesis and BCH decoding. *IEEE Trans. Inf. Theory* 15, 122-127 (1969).

- [14] Sun, Y., Yan, T., Li, H.: The linear complexity of a class of binary sequences with three-level autocorrelation. IEICE Trans. Fundamentals E96-A, 1586-1592 (2013).
- [15] Tang, X., Ding, C.: New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation Value. IEEE Trans.Inf. Theory 56, 6398-6405 (2010).
- [16] Tang, X., Fan, P., Matsufuji, S.: Lower bounds on the maximum correlation of sequences with low or zero correlation zone. Electron. Lett. 36, 551-552 (2000).
- [17] Tian, T., Qi, W.: 2-Adic complexity of binary m -sequences. IEEE Trans. Inf. Theory 56, 450-454 (2010).
- [18] Wang, Q.: The linear complexity of some binary sequences with three-level autocorrelation. IEEE Trans. Inf. Theory 56, 6388-6397 (2010).
- [19] Wang, Q., Du, X.: The linear complexity of binary sequences with optimal autocorrelation. IEEE Trans. Inf. Theory 56, 6388-6397 (2010).
- [20] Wang, Q., Jiang, Y., Lin, D.: Linear complexity of binary generalized cyclotomic sequences over $GF(q)$. Journal of Complexity 31, 731-740 (2015).
- [21] Xiong, H., Qu, L., Li, C., Fu, S.: Linear complexity of binary sequences with interleaved structure. IET Communications 7, 1688-1696 (2013).
- [22] Xiong, H., Qu, L., Li, C.: A new method to compute the 2-adic complexity of binary sequences. IEEE Trans. Inf. Theory 60, 2399-2406 (2014).
- [23] Xiong, H., Qu, L., Li, C.: 2-Adic complexity of binary sequences with interleaved structure. Finite Fields and Their Applications 33, 14-28 (2015).
- [24] Zhou, Z., Tang, X., Gong, G.: A new classes of sequences with zero or low correlation zone based on interleaving technique. IEEE Trans.Inf. Theory 54, 4267-4273 (2008).